CLAIMS

What is claimed is:

1. In a communication system having a plurality of networks, a method of achieving network separation between first and second networks comprising:

defining the first network with a first degree of trust;

defining the second network with a second degree of trust that is lower than the first degree of trust;

enabling communication between first and second networks via a network interface system using a communication protocol implemented in an application layer of a communication protocol stack; and

enabling data communication from the second network to the first network while minimizing data communication from the first network to the second network.

2. The method of claim 1, further comprising:

enabling applications operating on the second network to pass information to applications operating on the first network; and

configuring the network interface system into first and second regions for performing respective processing tasks of the first and second networks.

3. The method of claim 2, wherein the configuring includes implementing the network interface system with distinct sets of first and second processors, the first and second processors having a shared memory.

4. The method of claim 3, further comprising:

defining addresses in a user configuration table of the network interface system;

accepting information sent from the second network and only from addresses matching the addresses defined in the user configuration table;

configuring a protocol for use with the network interface system such that only valid connection requests are initiated via the protocol.

5. The method of claim 4, wherein the network interface system protocol enforces connection limits on data transfer to prevent saturation of the network interface system by a connection initiated from the second network.

6. The method of claim 4, further comprising:

enabling communications between the first and second regions via an interprocessor communication channel;

enabling data communication from the second network to the first network via the interprocessor communication channel;

configuring the interprocessor communication channel to communicate moving averages from the first network to the second network; and

configuring the network interface system to prevent the shared memory from overflowing by controlling the rate at which messages are acknowledged by the network interface system.

7. The method of claim 6, wherein the rate of acknowledgments is probabilistic, derived from a mean rate based on a moving average of the rate at which the first network is accepting messages from the second network.

8. The method of claim 4, further comprising:

configuring an application program loaded in the network interface system to support the protocol such that each application on the first and second networks using the network interface system communicates with a first and second application program interfaces, respectively, of the first and second networks.

9. The method of claim 8, further comprising:

accepting acknowledgments, at the application protocol layer, for messages transmitted from the network interface system to the first network;

communicating acknowledgment data from the network interface system to the second application program interface, the acknowledgments delivered in a fixed, predefined format; and

wherein, the acknowledgments provided to the second application program interface indicates that the network interface system successfully received data to be transmitted and stored in the shared memory, and wherein the acknowledgment data is generated by the network interface system.

10. The method of claim 9 wherein, for each active connection, a distinct variable is maintained that reflects a moving average of the time it takes for the first application program interface to accept messages from the second network;

randomly delaying messages received from the second application program interface over the active connection based on the moving average using a random variable of a pseudo-exponential or similar type; and

receiving messages at the application layer, wherein information flow from the first application program interface to the second application program interface occurs through changes in values of the moving average.

11. A network separation method for achieving network separation between first and second networks of a communication system, comprising:

providing a computer server configured to have a communication protocol stack implemented in an application layer; and

enabling data communication from the second network to the first network via the computer server, the first network having a higher degree of trust than the second network, and wherein rate of acknowledgment of messages by the computer server is probabilistic derived from a mean rate based on a moving average of the rate at which the first network accepts messages sent from the second network.

12. The method of claim 11, further comprising:

configuring the server into first and second regions for performing respective processing tasks of the first and second networks, wherein the configuring includes implementing the server with distinct sets of first and second processors and distinct sets of first and second memory, and the first and second processors having a shared memory;

defining addresses in a user configuration table configured in the server; and

accepting information sent from the second network and only from addresses matching the addresses defined in the user configuration table.

13. The method of claim 12, further comprising:

configuring a communication protocol for use with the server such that only valid connection requests are initiated via the protocol, and wherein the server is

configured to communicate moving averages from the first network to the second network, and wherein the protocol is configured to enforce connection limits on data transfer to prevent saturation of the server by a connection initiated from the second network.

14. A system for achieving network separation between first and second networks of a communication system, comprising:

a first processor for processing information from the first network;

a second processor for processing information from the second network, the first network having a higher degree of trust than the second network; and

wherein a rate of acknowledgment of messages by the system is probabilistic derived from a mean rate based on a moving average of the rate at which the first network accepts messages sent from the second network.

15. The system of claim 14, further comprising:

an interface configured to enable communications from the second network to the first network, and selectively route information from the first network to the second network;

a communication protocol stack implemented in an application layer; and

first and second application program interfaces configured to interface with application programs of first and second networks, respectively.

16. The system of claim 15, wherein the first processor has first memory, the second processor has second memory, and the first and second processors have a shared memory.

17. The system of claim 16, wherein the configuration table, having address information such that the first network is configured to accept information sent from the second network only from addresses matching the addresses defined in the user configuration table is provided from the first processor and first memory to the second processor and second memory through the shared memory.

18. The system of claim 17, wherein the protocol enforces connection limits on data transfer to prevent saturation of the system by a connection initiated from the second network, and wherein the interface is configured to communicate a value based on the moving averages from the first network to the second network, and to prevent the high memory from overflowing by controlling the rate at which messages are acknowledged by the system.

19. The system of claim 19, wherein for each active connection, the system maintains a distinct variable that reflects a moving average of the time it takes for the first application program interface to accept messages from the second network, and

messages received from the second application program interface are delayed based on the moving average using a random variable of a pseudo-exponential or similar type, and further wherein information flow from the first application program interface to the second application program interface occurs through changes in the moving average values.

20. A network separation system for achieving network separation between first and second networks of a communication system, comprising:

means for providing a computer server configured to have a communication protocol stack implemented in an application layer; and

means for enabling data communication from the second network to the first network via the computer server, the first network having a higher degree of trust than the second network, and wherein the rate of acknowledgment of messages by the computer server is probabilistic with a mean rate based on a moving average of the rate at which the first network accepts messages sent from the second network.